**CSCI 2312: Discrete Structures II: Modular Arithmetic Part II**

**Theorem:**

$$x \equiv_m y \Leftrightarrow (x \; rem \; m) = (y \; rem \; m)$$

Proof:

By the remainder theorem, $\exists! q_x, q_y, r_x, r_y \in \mathbb{Z}$ such that $0 \leq r_x, r_y < m$, $x = q_x m + r_x$ and $y = q_y m + r_y$.

$\Rightarrow$:

$$x \equiv_m y \Rightarrow m \mid (y - x) \Rightarrow \exists c \in \mathbb{Z} \; such \; that \; (y - x) = cm$$

$$\Rightarrow (q_y - q_x)m + (r_y - r_x) = cm \Rightarrow r_y - r_x = (c - q_y + q_x)m = dm \; for \; d \; \in \; \mathbb{Z}$$

Further, $-m < -r_x \leq 0$, hence $-m < r_y - r_x < m$. Hence $d = 0$ is the only possible value for $d$ and $r_y = r_x$ or $x \; rem \; m = y \; rem \; m$.

$\Leftarrow$:

$$x \; rem \; m = y \; rem \; m \Rightarrow r_x = r_y \Rightarrow x - q_x m = y - q_y m \Rightarrow y - x = (q_y - q_x)m \Rightarrow m \mid (y - x) \; as \; (q_y - q_x) \in \mathbb{Z}$$

Hence $x \equiv_m y$.